Week 7- Cloud vulnerability Scanning

Name- Samruddhi Dattu Nikam

PRN- 2124UCSF2019

Email- samruddhi.nikam_24ucs@sanjivani.edu.in

❖ TASK- 1) Scan cloud instances using free scanners.
2) Identify vulnerabilities.
3) Document remediation steps.

Step 1: Log in to AWS Console

- Go to AWS Management Console.
- Sign in with your AWS account.

Step 2: Open AWS Inspector

- In the **search bar** (top of AWS console), type **Inspector**.
- Click on **Amazon Inspector**.

Step 3: Enable Inspector (First-time setup)

- If this is your **first time**, you'll see a **Get started** or **Enable Amazon Inspector** button.
- Click **Enable** → Wait for AWS to activate it

Step 4: Select the Instances for Scanning

- Amazon Inspector automatically detects your **EC2 instances** and **container images**.
- You'll see your resources listed under **"Coverage"**.

Step 5: Run a Scan

- AWS Inspector scans automatically once enabled.
- If you want **manual scan**, click:
  - **Scans** → **Start scan** → Select resources → Click **Run**.

Step 6: View Vulnerability Findings

- Go to **Findings** tab.

Week 7- Cloud vulnerability Scanning

- You'll see a list of vulnerabilities:
  - **Severity**: Critical, High, Medium, Low.
  - **Description**: What the issue is.
  - **Affected Resource**: The EC2 instance ID.
  - **Remediation**: How to fix it.

Step 7: Document the Findings

In your documentation, note:

- **Finding name**
- **Severity**
- **Affected Resource**
- **Recommendation**

Step 8: Apply Remediation

Typical remediation steps:

- **Outdated packages** → SSH into the EC2 instance and run:

```
bash
CopyEdit
sudo apt update && sudo apt upgrade -y   # For Ubuntu/Debian
sudo yum update -y                       # For Amazon Linux/RHEL
```

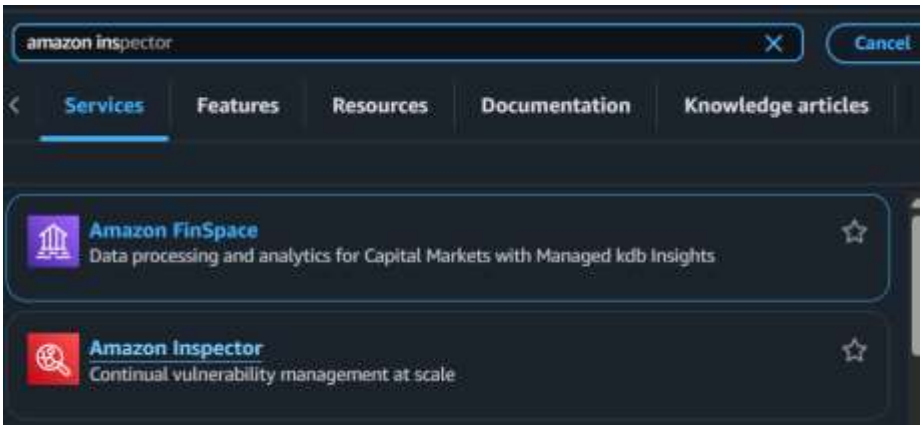
- **Unnecessary open ports** → Go to **EC2 → Security Groups** → Edit inbound rules → Remove unused ports.
- **Weak configurations** → Update IAM policies, use stronger encryption, etc.

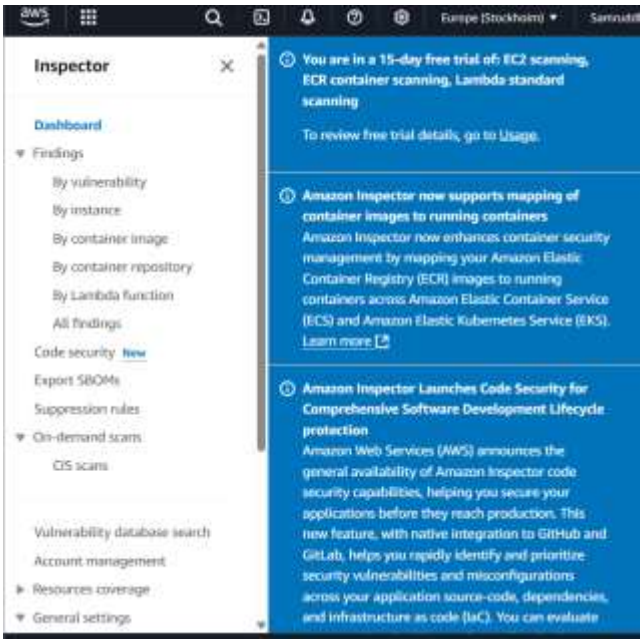
Step 9: Re-Scan After Fix

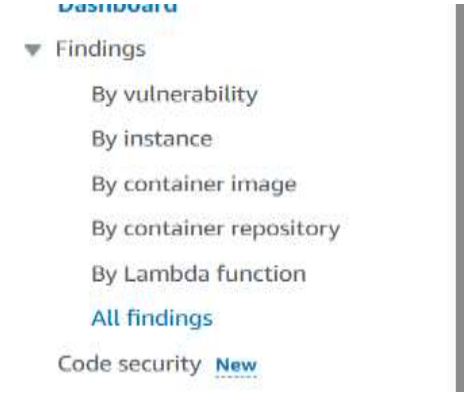
- Run another scan from **Inspector → Scans → Start Scan** to confirm vulnerabilities are resolved.

Week 7- Cloud vulnerability Scanning

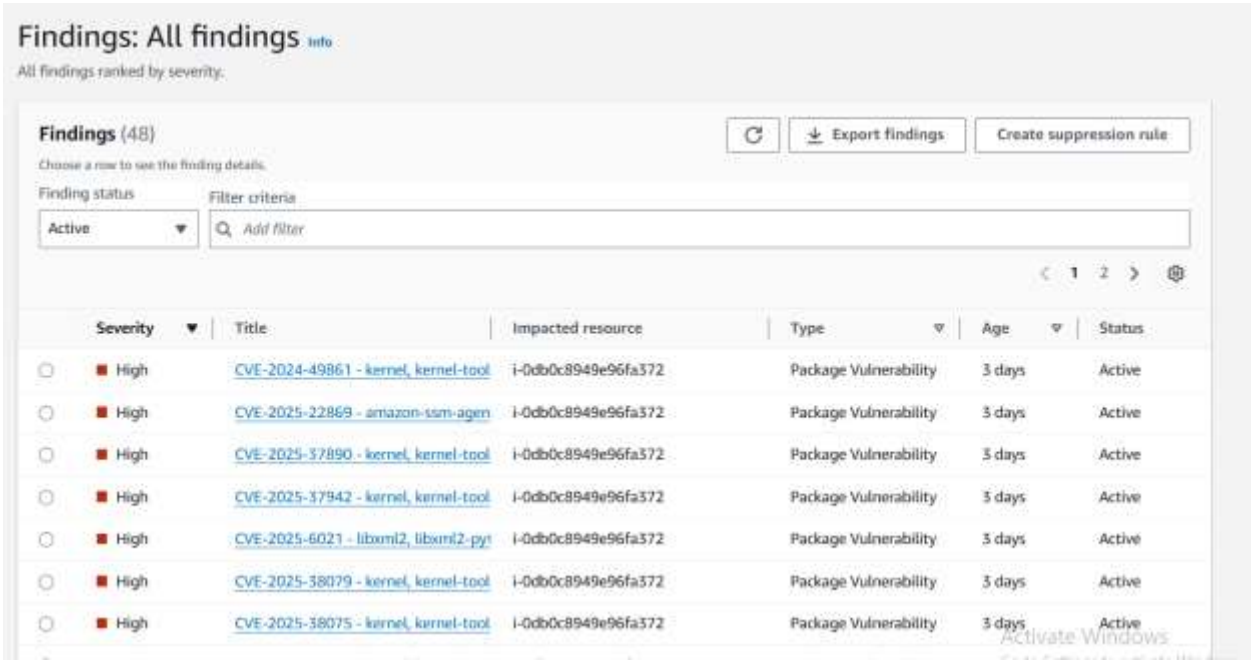
- Screenshot-

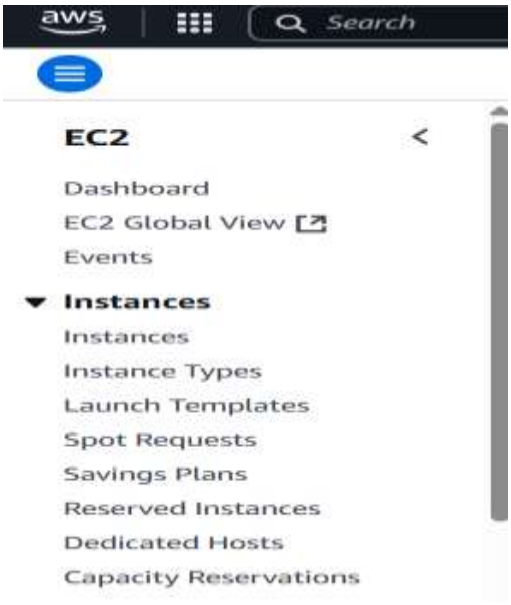






Week 7- Cloud vulnerability Scanning






```
Microsoft Windows [Version 10.0.22631.5699]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Shree>ssh -i ssh "C:\Users\Shree\Downloads\Mykeypair.pem"
Warning: Identity file ssh not accessible: No such file or directory.
ssh: Could not resolve hostname C:\\Users\\Shree\\Downloads\\Mykeypair.pem: No such host is known.

C:\Users\Shree>ssh -i "C:\Users\Shree\Downloads\Mykeypair.pem" ec2-user@ec2-16-170-242-131.eu-north-1.compute.amazonaw
The authenticity of host 'ec2-16-170-242-131.eu-north-1.compute.amazonaws.com (16.170.242.131)' can't be established.
ED25519 key fingerprint is SHA256:WIqa0pr+OdL1lAuqix/edcCcDM55sB+4sRFcmVSTZY4.
This host key is known by the following other names/addresses:
    C:\Users\Shree/.ssh/known_hosts:1: 16.170.242.131
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

Week 7- Cloud vulnerability Scanning

```
C:\Users\Shree>ssh -i "C:\Users\Shree\Downloads\Mykeypair.pem" ec2-user@ec2-16-170-242-131.eu-north-1.compute.amazonaws.com
The authenticity of host 'ec2-16-170-242-131.eu-north-1.compute.amazonaws.com (16.170.242.131)' can't be established.
ED25519 key fingerprint is SHA256:WIqa0pr+OdL1lAuqix/edcCcDM55sB+4sRFcmVSTZY4.
This host key is known by the following other names/addresses:
    C:\Users\Shree/.ssh/known_hosts:1: 16.170.242.131
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-16-170-242-131.eu-north-1.compute.amazonaws.com' (ED25519) to the list of known hosts.
Last login: Thu Jun  5 07:44:15 2025 from 152.57.57.253
       #_
   ~\_  ####_        Amazon Linux 2
  ~~  \_#####\
  ~~     \###|       AL2 End of Life is 2026-06-30.
  ~~       \#/ ___
   ~~       V~' '->
    ~~~         /    A newer version of Amazon Linux is available!
      ~~._.   _/
         _/ _/       Amazon Linux 2023, GA and supported until 2028-03-15.
       _/m/'           https://aws.amazon.com/linux/amazon-linux-2023/

28 package(s) needed for security, out of 30 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-46-230 ~]$
```

```
Installed:
  kernel.x86_64 0:5.10.239-236.958.amzn2

Updated:
  amazon-ssm-agent.x86_64 0:3.3.2299.0-1.amzn2            aws-cfn-bootstrap.noarch 0:2.0-35.amzn2          cloud-init.noarch 0:19.3-46.am
  kernel-tools.x86_64 0:5.10.239-236.958.amzn2            libicu.x86_64 0:50.2-4.amzn2.0.2                 libtasn1.x86_64 0:4.10-1.amzn2
  libxml2.x86_64 0:2.9.1-6.amzn2.5.19                     libxml2-python.x86_64 0:2.9.1-6.amzn2.5.19       mtr.x86_64 2:0.92-2.amzn2.0.2
  openssh.x86_64 0:7.4p1-22.amzn2.0.10                    openssh-clients.x86_64 0:7.4p1-22.amzn2.0.10     openssh-server.x86_64 0:7.4p1-
  perl.x86_64 4:5.16.3-299.amzn2.0.3                      perl-Pod-Escapes.noarch 1:1.04-299.amzn2.0.3     perl-libs.x86_64 4:5.16.3-299.
  perl-macros.x86_64 4:5.16.3-299.amzn2.0.3               python.x86_64 0:2.7.18-1.amzn2.0.13              python-devel.x86_64 0:2.7.18-1
  python-libs.x86_64 0:2.7.18-1.amzn2.0.13                python-requests.noarch 0:2.6.0-10.amzn2.0.7      python-urllib3.noarch 0:1.25.9
  python2-cryptography.x86_64 0:1.7.2-2.amzn2.0.1         python2-setuptools.noarch 0:41.2.0-4.amzn2.0.6   python3.x86_64 0:3.7.16-1.amzn
  python3-libs.x86_64 0:3.7.16-1.amzn2.0.18               python3-pip.noarch 0:20.2.2-1.amzn2.0.12         python3-setuptools.noarch 0:49
  screen.x86_64 0:4.1.0-0.27.20120314git3c2946.amzn2.0.2  sudo.x86_64 0:1.8.23-10.amzn2.3.8

Complete!
[ec2-user@ip-172-31-46-230 ~]$
```